(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
10 April 2003 (10.04.2003)

PCT

(10) International Publication Number
WO 03/030452 A2

(51) International Patent Classification[7]: H04L 12/18, 12/28, 29/12, G06F 9/46

(21) International Application Number: PCT/IB02/03778

(22) International Filing Date: 12 September 2002 (12.09.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/970,539 3 October 2001 (03.10.2001) US

(71) Applicant: KONINKLIJKE PHILIPS ELECTRONICS N.V. [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventor: MOONEN, Jan, R.; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL.).

(74) Agent: GROENENDAAL, Antonius, W., M.; Internationaal Octrooibureau B.V., Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

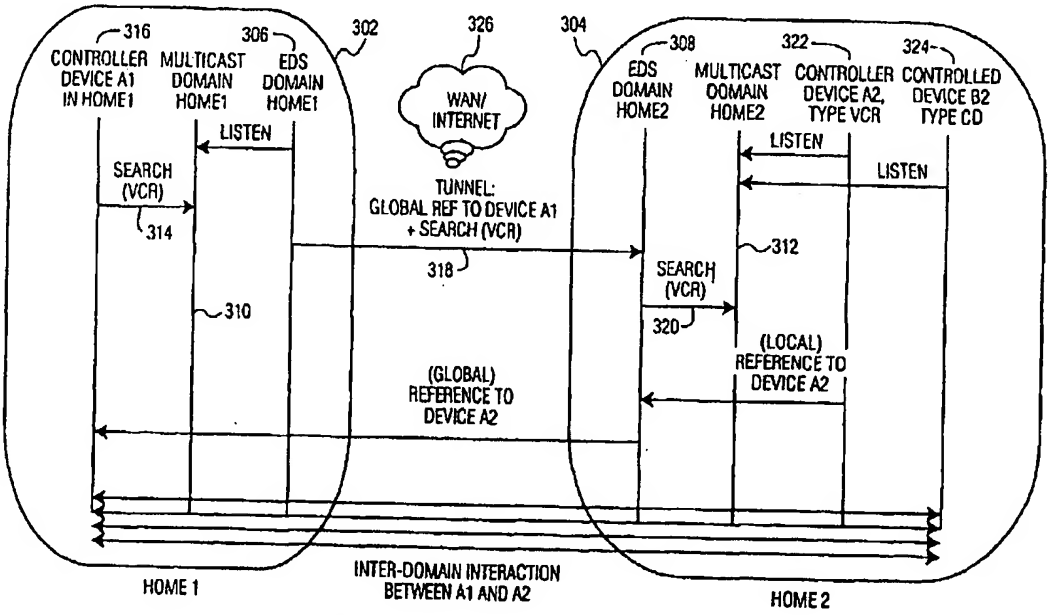
(81) Designated States *(national)*: CN, JP.

(84) Designated States *(regional)*: European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: MULTICAST DISCOVERY PROTOCOL USES TUNNELING OF UNICAST MESSAGE



(57) Abstract: The scope of discovery protocols on network domains of devices and services is extended. A search message or an announcement message on a multicast channel in one domain gets encapsulated into a unicast message that is sent to a second domain. The multicast message is extracted from the unicast message in the second domain and is input to the second domain's multicast channel.

WO 03/030452 A2

Multicast discovery protocol uses tunneling of unicast message

The invention relates to aspects and use of discovery procedures on a multi-domain network.

Home network architectures such as HAVi, UPnP, Jini and VESA typically contain a device discovery protocol. This protocol is used to implement plug-and-play behavior, i.e., when a device is plugged into the network (or - in the wireless case - comes within range) it is automatically discovered by all interested parties, and can be used immediately. IP-based home networks such as UPnP and Jini build their discovery protocol on top of IP multicasting. In this case, a standard IP address and port are standardized as the multicast channel. Devices that join the network and want to announce themselves to the rest of the network send certain announcement messages to this channel. Devices that want to discover new devices simply listen to this channel.

Automatic discovery of devices is particularly important for wireless devices such as PDAs or mobile phones that enter or leave the (home) network, together with the person carrying them. However, automatic discovery is also relevant to non-mobile devices. These devices may be turned on or off by users at will, and in that sense enter or leave the network. Another reason why automatic discovery is important is the volatile nature of IP addresses. Typically, IP address allocation schemes such as DHCP assign IP addresses to devices on a temporary basis. In other words, a device discovered yesterday at IP address "A" might have IP address "B" tomorrow. The discovery protocol offers a mechanism for this device to announce itself at this new address, thereby ensuring that all interested clients become aware of this new address. Even if the device has not left or entered the home network from a *user* point of view, it has from a *network* point of view. Hence, discovery is not just a one-time-only activity performed when a device is brought home from a store and placed into a home network. Rather, it is a setup process that needs to be performed every time a user or application wants to use and control certain types of devices.

Discovery based on IP multicasting gives rise to some problems. For example, IP multicasting is not generally supported throughout the whole Internet. Many IP routers and firewalls/gateways simply block all multicast traffic. As another problematic aspect, IP multicasting does not scale. A multicast message needs to have a Time-To-Live (TTL) field

specifying the scope of the multicast message. The TTL field specifies the number of routers that this packet may traverse, and is needed to avoid flooding the whole Internet with these messages. The IP multicast routing protocol uses the TTL field of IP datagrams to decide how "far" from a sending host a given multicast packet should be forwarded. The default TTL for multicast datagrams is unity, which results in multicast packets going only to other hosts on the local network. It is generally impossible to know the number of routers in a path between two devices. Hence is it generally unknown to predict a sensible TTL value, and there is no guarantee in advance that a multicast message will reach all relevant destinations.

The inventor has realized that a TTL value can be used to specify clusters of devices that can discover each other. An aspect of this invention relates, among other things, to a mechanism to connect multiple ones of such clusters via "tunneling" of these multicast messages inside point-to-point (or unicast) messages exchanged between Extended Discovery Servers. The result is that devices and applications in separate clusters, residing at locations remote from each other and connected through these servers, can now discover and control each other.

An aspect of the invention therefore relates to a method of bridging a plurality of multicast domains. A multicast message, originating in a specific one of the domains, is enabled to be transferred as a unicast message to at least another one of the domains. Then, the multicast message is enabled to be re-generated from the unicast message in the other domain.

Another aspect of the invention relates to hardware or a software component for use on a first multicast domain, e.g., a first part of a home network. The component is operative to encapsulate a multicast message in a unicast message for being sent to a second multicast domain, e.g., a second part of the home network.

The invention allows to extend the scope of discovery protocols via multicast tunneling and reference translation: a search message or an announcement message on a multicast channel in one domain gets encapsulated into a unicast message that is sent to a second domain. The multicast message is extracted from the unicast message in the second domain and is input to the second domain's multicast channel.

The invention is explained below in further detail, by way of example, and with reference to the accompanying drawings, wherein:

Figs. 1 and 2 are event diagrams illustrating searching and announcement events in a multicast domain;

Figs. 3 and 4 are event diagrams illustrating the tunneling of a multicast messages between two multicast domains;

Figs. 5 and 6 are event diagrams illustrating the tunneling between multicast domains with a UPnP configuration.

Throughout the figures, same reference numerals indicate similar or corresponding components or features.

Figs. 1 and 2 are event diagrams illustrating searching and announcing events in a single multicast domain. A typical discovery protocol involves devices (or software applications) that assume one of two possible roles: on the one hand a controlled device or server; and on the other hand a controller device or client application. A discovery protocol implements active searching by controller devices for controlled devices (of a particular type).

In Fig. 1, a controller device 102 sends a search message 104 to a multicast channel 106. Controlled devices 108, 110 and 112 listen to multicast channel 106. Relevant ones of controlled devices 108-112 send unicast responses 114 and 116 to device 102, the sender of search message 104.

In Fig. 2, controlled devices 108 and 208 send announcement messages 202 and 204 to multicast channel 106 to announce their presence, e.g., periodically or upon a certain event such as "power-on" or "coming within range" as for device 208. Controlled device 110 sends announcement messages 206, to multicast channel 106 to announce its imminent disappearance (e.g., in case of a power shutdown).

Search responses 114 and 116 and presence announcements 202 and 204 contain respective references to the respective discovered devices. A reference comprises, e.g., an IP address or a URL. Subsequent interaction with the discovered device is based on this reference.

This invention introduces a software component referred to herein as an "Extended Discovery Server" (EDS) that can be added to a (home) network in order to enable the devices on this network to discover (or be discovered) and be used by remote devices. The EDS needs to be connected, through the Internet or another Wide Area Network (WAN), to one or more remote EDSs. It needs to know global references to these EDSs, such

as static global IP addresses or registered Internet domain names. The operation of an EDS is described below for two scenarios: a controller device searches for remote devices to interact with, and a controlled device announces its presence or imminent disappearance to remote controller devices.

Fig. 3 illustrates a scenario with events in a domain 302 and a domain 304, e.g., Home1 and Home2, respectively. Domain 302 has an EDS 306 and domain 304 has an EDS 308. EDSs 306 and 308 enable to share their networks, i.e., domains 302 and 304, with one another. EDSs 306 and 308 both listen to messages on multicast channels 310 and 312. In the example shown, a search message 314 is detected by EDS 306 in domain 302. EDS 306 encapsulates multicast message 314 together with a reference to the multicast sender, here a device 316, in a new unicast message 318. In case original multicast sender 316 in domain 302 was using a local reference, that reference is translated via, for example, NAT, and replaced by an equivalent global reference. EDS 306 then sends encapsulated multicast message 318 as unicast message via WAN 326 to one or more other EDSs that it wants to share devices with. In this example, the relevant other EDS is EDS 308. When EDS 308 receives message 318 from EDS 306, the former extracts the encapsulated search message 314 and the global reference of original multicast sender 316. EDS 308 then sends extracted search message 320 to a multicast channel 312 in domain 304. Thus, original multicast message 314 is regenerated in a different multicast domain as if it has tunneled from domain 302 via WAN 326 into domain 304. Since EDS 308 is the sender of regenerated multicast message 320, it will receive the response, if any, to this search message. Each response received from devices in domain 304, e.g., devices 322 and 324, will be forwarded to sender 316 of the original search in domain 302. In case the responses contain local references, those references are translated via, for example, NAT, and replaced by equivalent global references. Now that controller device 316 in domain 302 has discovered controlled device 322 in domain 304 that it searched for, it can use the reference received to interact with device 322. The actual mechanism to implement this is independent of this invention. Usually, these mechanisms are based on unicast, such as HTTP.

Fig. 4 illustrates a scenario with events in domains 302 and 304, wherein a device 406 announces its presence. EDSs 306 and 308 listen to messages on the standardized multicast channels 310 and 312, respectively. Whenever an announcement message 404 is detected by an EDS, in this scenario by EDS 308 in domain 304, the relevant EDS encapsulates the entire multicast message 404. In case announcement 404 contains a local reference, e.g., to its sender device 406, that reference is translated via, for example, NAT

and replaced by an equivalent global reference. EDS 308 then sends the encapsulated multicast message 408 as unicast message via WAN 326 to one or more other EDSs, in this scenario, EDS 306. When EDS 306 receives unicast message 408 from EDS 308, the former extracts encapsulated announcement message 404 from message 408. EDS 306 then sends the extracted announcement message 412 to multicast channel 310 in domain 302. Thus, original multicast message 404 is regenerated in a different multicast domain as if it had tunneled from domain 304 via WAN 326 to domain 302. Now that announcement 404 has been regenerated in domain 302 as message 412, controller devices in domain 302 are aware of new device 406 in domain 304 and can interact with device 406 through the reference contained in announcement message 412. The actual mechanism to do this is independent of this invention. Usually, these mechanisms are based on unicast, such as HTTP.

The invention allows entities that can be discovered within a single domain, e.g., a home network or another restricted area, to be discovered by remote applications, in a controlled way. The entities can be devices such as those based on UPnP, services, individual pieces of audio/video (AV) content information, or even persons associated with a personal device such as a PDA or mobile phone. The reach of the extended discovery protocol is determined by the set of EDSs that know each other's network address.

For example, a group of three friends might decide to share their home network by establishing a relation between their EDSs. Another example is a mobile professional that establishes a relation between his EDS at home and his EDS at work or vacation location. The actual mechanism to establish these relations is independent of the object of this invention.

After discovery of a remote entity through the EDS mechanism, the entity may be used/controlled. For example: a security camera in a home may be inspected from a work or vacation location; a song or video stored in a friends home may be downloaded or streamed to your own home; a VCR in a home may be programmed from a remote location; a device may be turned off from a remote location, to save energy; one's home network can be monitored remotely to detect intrusions/abnormalities such as devices disappearing without authorization or applications searching for devices at odd times of the day.

An EDS may implement a filtering mechanism, to allow remote access only to certain devices in the home, or only at certain times of the day, or only to certain 'trusted' remote EDSs. This filtering can also be personalized per user.

Figs. 5 and 6 illustrate the above in some more detail for multicast domains with UPnP configurations. The UPnP standard defines a discovery protocol referred to as

Simple Service Discovery Protocol (SSDP). It is used to discover either UPnP devices or UPnP services. In UPnP terminology, a service is a functional component that is part of a UPnP device. SSDP uses a standard multicast channel, 239.255.255.250:1900, and a TTL of 4. SSDP defines the following messages:

- NOTIFY(ssdp:alive) : periodically sent by a controlled device to the multicast channel to announce its presence. Contains a URL reference to the devices' description document.

- NOTIFY(ssdp:byebye) : sent by a controlled device to the multicast channel to announce its imminent disappearance.

- M-SEARCH (<search-target>) : sent by a controller device to the multicast channel to search for specific device types, service types, device instances or all devices. Controlled devices that match the <search target> need to respond to the sender of the search with a message containing a URL reference to the device's description document.

After a controller device has used SSDP to discover a device that it is interested in, it has the URL to the device's document. It can subsequently fetch this document and parse it to find references to the services (= functional components) that the device contains. It can then use those references to actually interact with this device. The references are in the form of URLs, and interaction is based on using the HTTP protocol (via a POST message) between controller device and controlled device.

In some homes, the URL references that a device uses to announce itself are based on a so-called 'local' IP address, meaning that the address is not globally unique, and the URL reference is not usable on the global Internet. In such a home, at least one device – e.g., the Internet Gateway – has a global IP address. This Internet Gateway typically implements NAT (Network Address Translation) or NAPT (Network Address Port Translation), which is a mechanism to map a local IP address plus port to a global IP address plus port. The EDS can use this mechanism to replace local addresses by a global address for all SSDP messages that leave the home to travel the Internet and arrive at a remote home. Specifically, this concerns the following messages:

- NOTIFY(ssdp:alive) of a local device;

- response to a remote M-SEARCH (<search-target>) message;

In this embodiment, the unicast message used to tunnel is an HTTP POST mechanism. The HTTP body contains the complete SSDP message (the SSDP header + body) plus, in case of an SSDP search, the IP address and port of the sender. This latter

information is encoded as an HTTP header called 'ORGINAL-MCAST-SENDER'. The EDSs in this embodiment know each other, in the form of a URL reference.

More specifically, a tunneled search message looks like this:

```
POST <path of URL of EDS> HTTP/1.1
M-SEARCH * HTTP/1.1
HOST: 239.255.255.250:1900
MAN: "ssdp:discover"
MX: <seconds to delay response>
ST: <search target>
ORGINAL-MCAST-SENDER: <global IP address and port of the multicast sender>
```

A tunneled announcement of presence message looks like this:

```
POST <path of URL reference of remote EDS> HTTP/1.1
NOTIFY * HTTP/1.1
HOST: 239.255.255.250:1900
CACHE-CONTROL: max-age = <seconds until advertisement expires>
LOCATION: <global URL reference to the device>
NT: <search target>
NTS: "ssdp:alive"
SERVER: <OS/version> UPnP/1.0 <product/version>
USN: <advertisement UUID>
```

A tunneled announcement of imminent disappearance message may look like:

```
POST <path of URL of EDS> HTTP/1.1
NOTIFY * HTTP/1.1
HOST: 239.255.255.250:1900
NT: <search target>
NT: "ssdp:byebye"
USN: <advertisement UUID>
```

The HTTP POST response to this would be a standard ok response, in all cases:

```
HTTP/1.1 200 OK
```

Parts of the above messages that are enclosed in brackets ("<" and ">") are not to be taken literally, but are to be interpreted as defined in the UPnP SSDP specification.

Figs. 5 and 6 are event diagrams showing the scenarios for search tunneling corresponding to Fig. 3, and for announcement tunneling corresponding to Fig. 4. The events have been rephrased in terms specific to this UPnP/SSDP/HTTP embodiment.

CLAIMS:

1. A method of bridging a plurality of multicast domains, the method comprising:

- enabling to transfer a multicast message, originating in a specific one of the domains, as a unicast message to at least another one of the domains;
- enabling to regenerate the multicast message from the unicast message in the other domain.

2. The method of claim 1, wherein the multicast message comprises a search message for discovery of a device or service.

3. The method of claim 1, wherein the multicast message comprises an announcement message for announcing the presence of a device or service.

4. The method of claim 1, wherein at least part of the specific domain or the other domain forms part of a wireless network.

5. The method of claim 1, using IP multicasting.

6. The method of claim 1, wherein at least one of the domains has a UPnP architecture.

7. A unicast message on a data network, a multicast message being encapsulated in the unicast message.

8. A component for use with a multicast domain, the component being operative to encapsulate a multicast message, received from a multicast channel in the multicast domain, in a unicast message.

9. A component for use with a multicast domain, the component being operative to extract a multicast message from a unicast message for forwarding the multicast message to a multicast channel of the multicast domain.

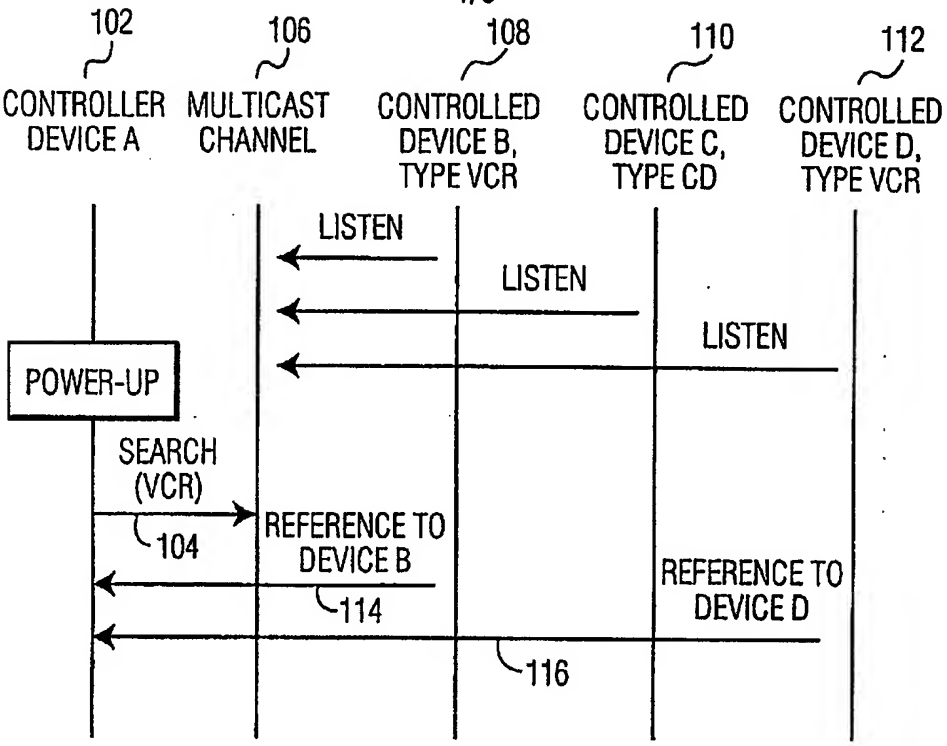

102
106
108
110
112
CONTROLLER DEVICE A
MULTICAST CHANNEL
CONTROLLED DEVICE B, TYPE VCR
CONTROLLED DEVICE C, TYPE CD
CONTROLLED DEVICE D, TYPE VCR
LISTEN
LISTEN
LISTEN
POWER-UP
SEARCH (VCR)
104
REFERENCE TO DEVICE B
114
REFERENCE TO DEVICE D
116

FIG. 1

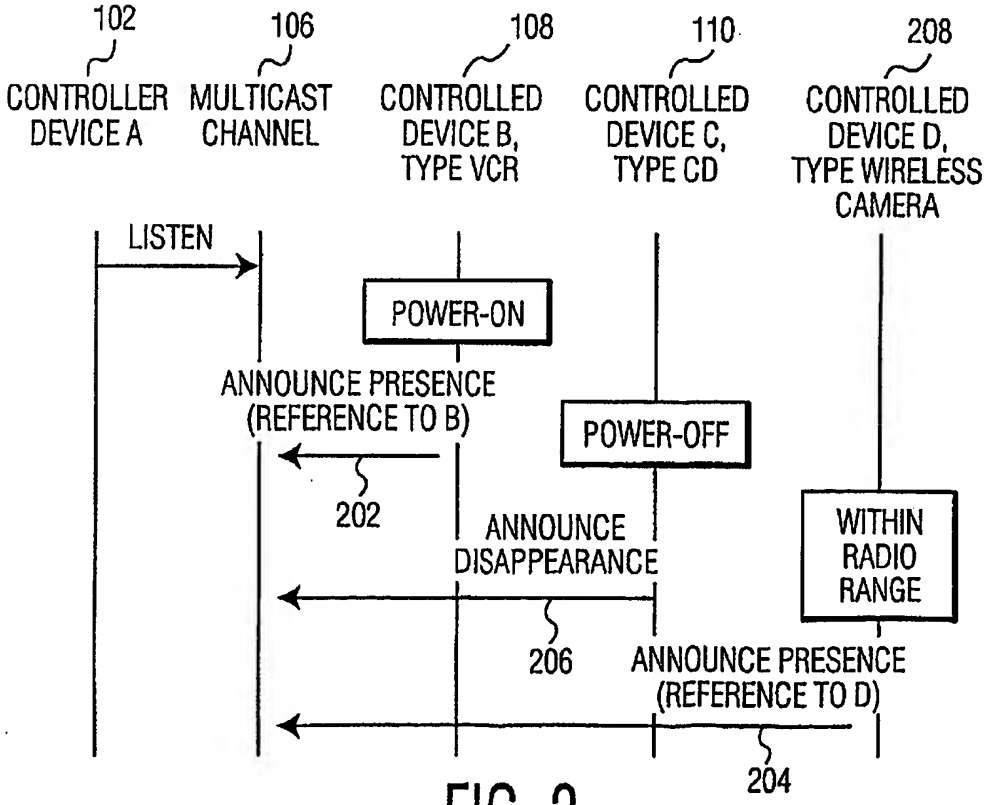

102
106
108
110
208
CONTROLLER DEVICE A
MULTICAST CHANNEL
CONTROLLED DEVICE B, TYPE VCR
CONTROLLED DEVICE C, TYPE CD
CONTROLLED DEVICE D, TYPE WIRELESS CAMERA
LISTEN
POWER-ON
ANNOUNCE PRESENCE (REFERENCE TO B)
202
POWER-OFF
ANNOUNCE DISAPPEARANCE
206
WITHIN RADIO RANGE
ANNOUNCE PRESENCE (REFERENCE TO D)
204

FIG. 2

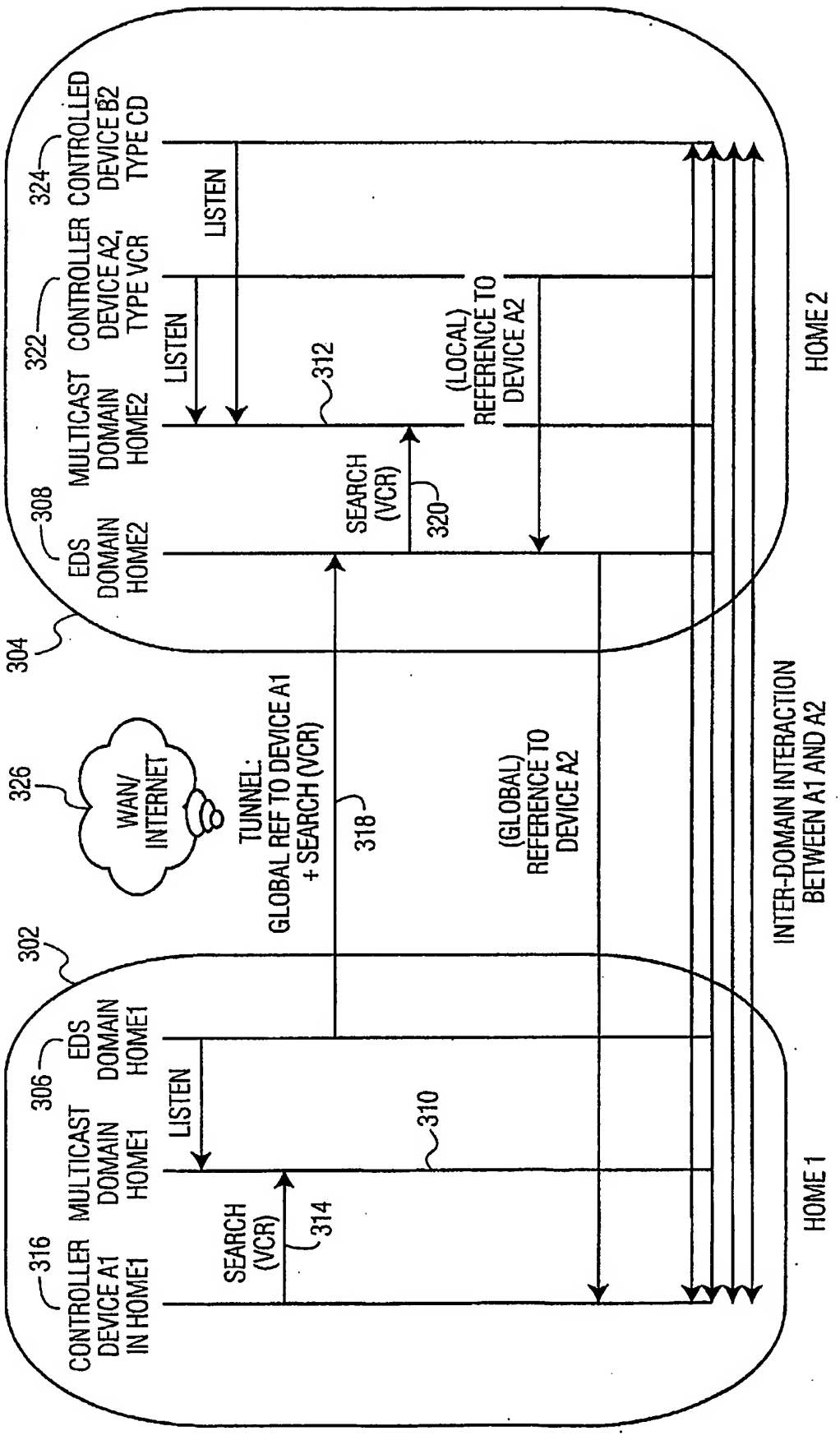

302
HOME 1
316
CONTROLLER DEVICE A1 IN HOME1
MULTICAST DOMAIN HOME1
306
EDS DOMAIN HOME1
LISTEN
SEARCH (VCR)
314
310
304
HOME 2
308
EDS DOMAIN HOME2
MULTICAST DOMAIN HOME2
322
CONTROLLER DEVICE A2, TYPE VCR
324
CONTROLLED DEVICE B2 TYPE CD
LISTEN
LISTEN
312
SEARCH (VCR)
320
(LOCAL) REFERENCE TO DEVICE A2
326
WAN/ INTERNET
TUNNEL: GLOBAL REF TO DEVICE A1 + SEARCH (VCR)
318
(GLOBAL) REFERENCE TO DEVICE A2
INTER-DOMAIN INTERACTION BETWEEN A1 AND A2

FIG. 3

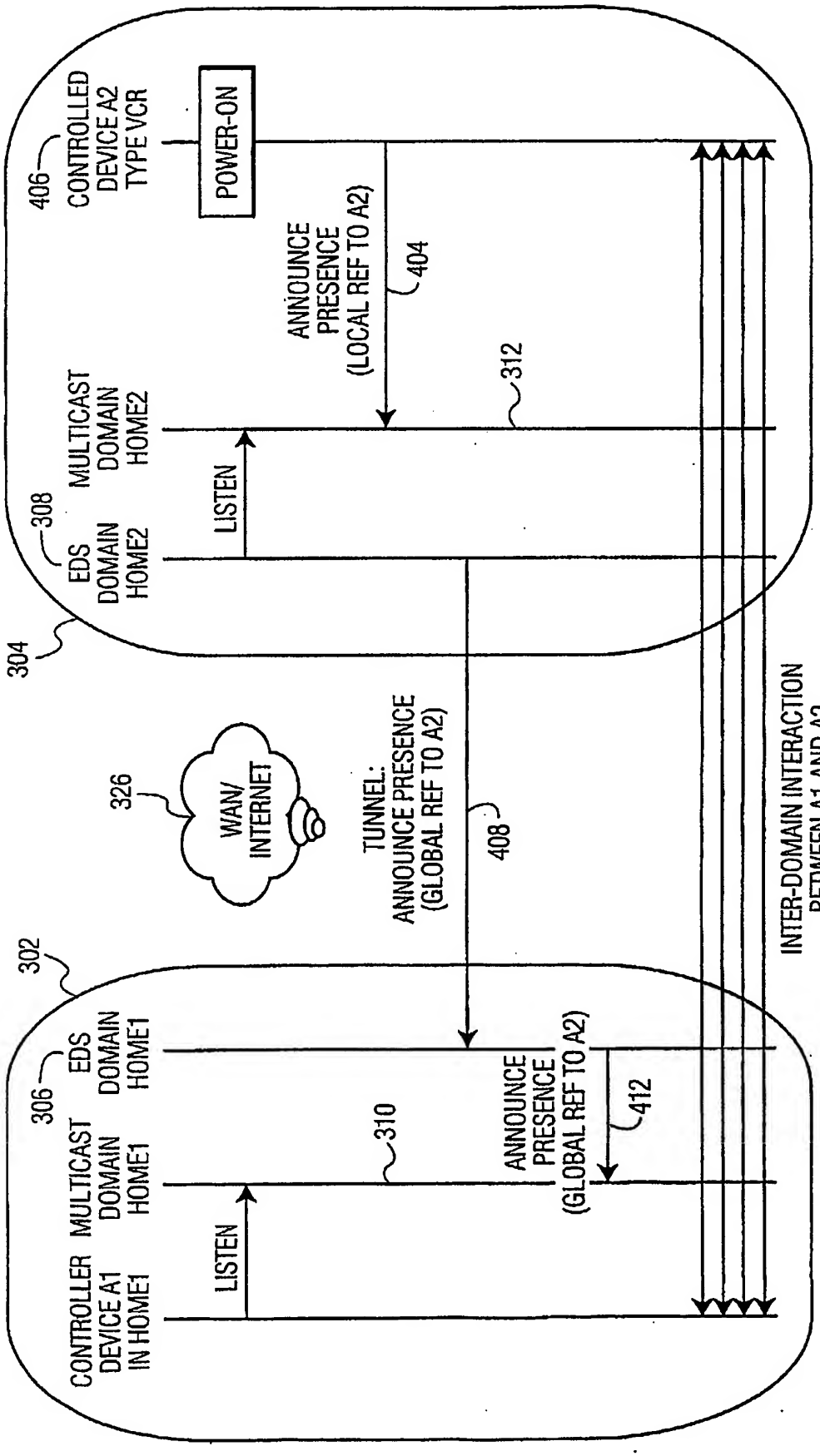

CONTROLLER DEVICE A1 IN HOME1
MULTICAST DOMAIN HOME1
306
EDS DOMAIN HOME1
302
LISTEN
310
ANNOUNCE PRESENCE (GLOBAL REF TO A2)
412
TUNNEL: ANNOUNCE PRESENCE (GLOBAL REF TO A2)
408
WAN/ INTERNET
326
INTER-DOMAIN INTERACTION BETWEEN A1 AND A2
EDS DOMAIN HOME2
308
MULTICAST DOMAIN HOME2
LISTEN
312
ANNOUNCE PRESENCE (LOCAL REF TO A2)
404
CONTROLLED DEVICE A2 TYPE VCR
406
POWER-ON
304

FIG. 4

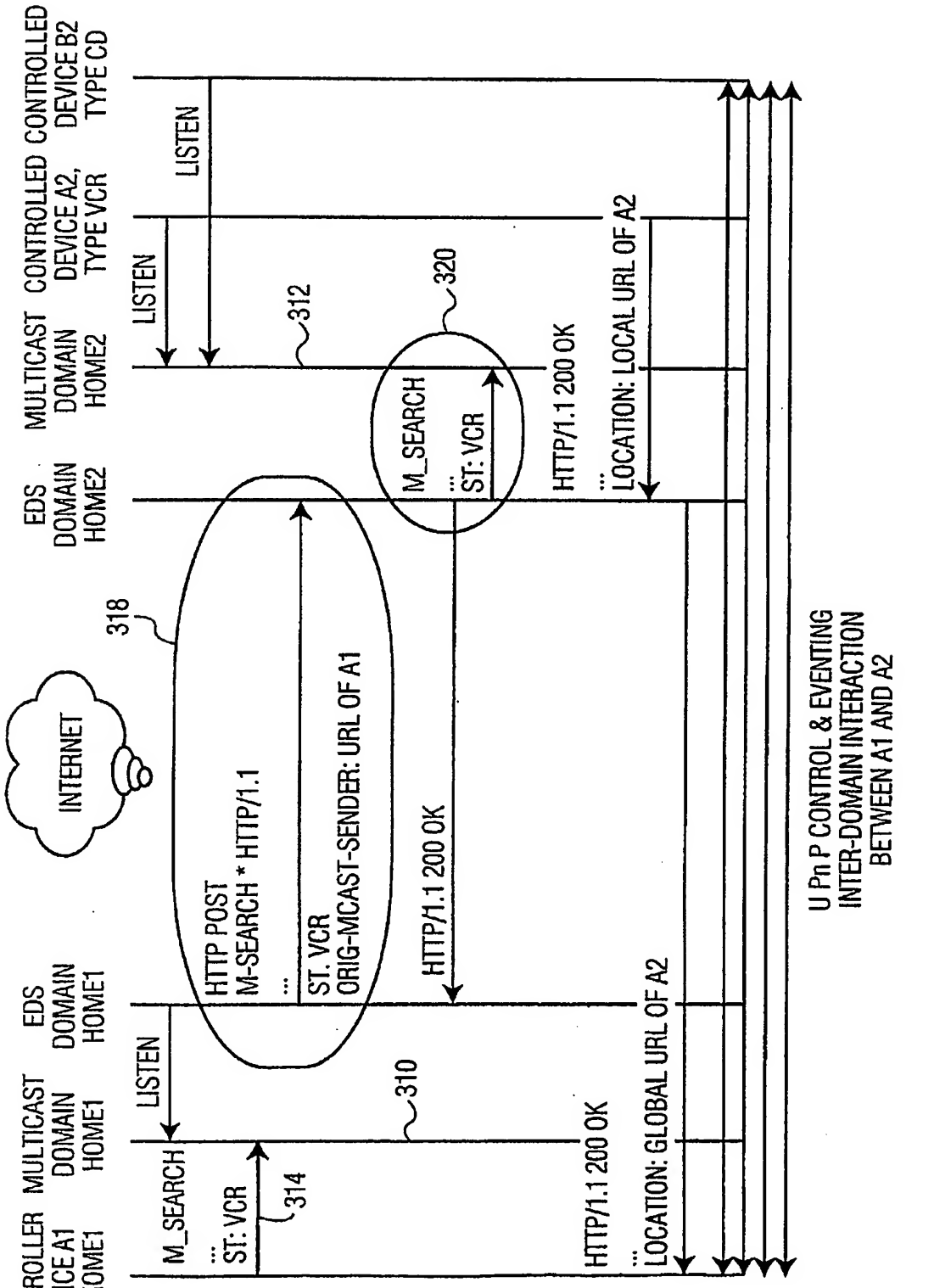

CONTROLLER DEVICE A1 IN HOME1
MULTICAST DOMAIN HOME1
EDS DOMAIN HOME1
INTERNET
EDS DOMAIN HOME2
MULTICAST DOMAIN HOME2
CONTROLLED DEVICE A2, TYPE VCR
CONTROLLED DEVICE B2 TYPE CD
LISTEN
M_SEARCH
ST: VCR
314
310
HTTP/1.1 200 OK
LOCATION: GLOBAL URL OF A2
318
HTTP POST M-SEARCH * HTTP/1.1
ST. VCR
ORIG-MCAST-SENDER: URL OF A1
HTTP/1.1 200 OK
312
320
M_SEARCH
ST: VCR
HTTP/1.1 200 OK
LOCATION: LOCAL URL OF A2
U Pn P CONTROL & EVENTING INTER-DOMAIN INTERACTION BETWEEN A1 AND A2

FIG. 5

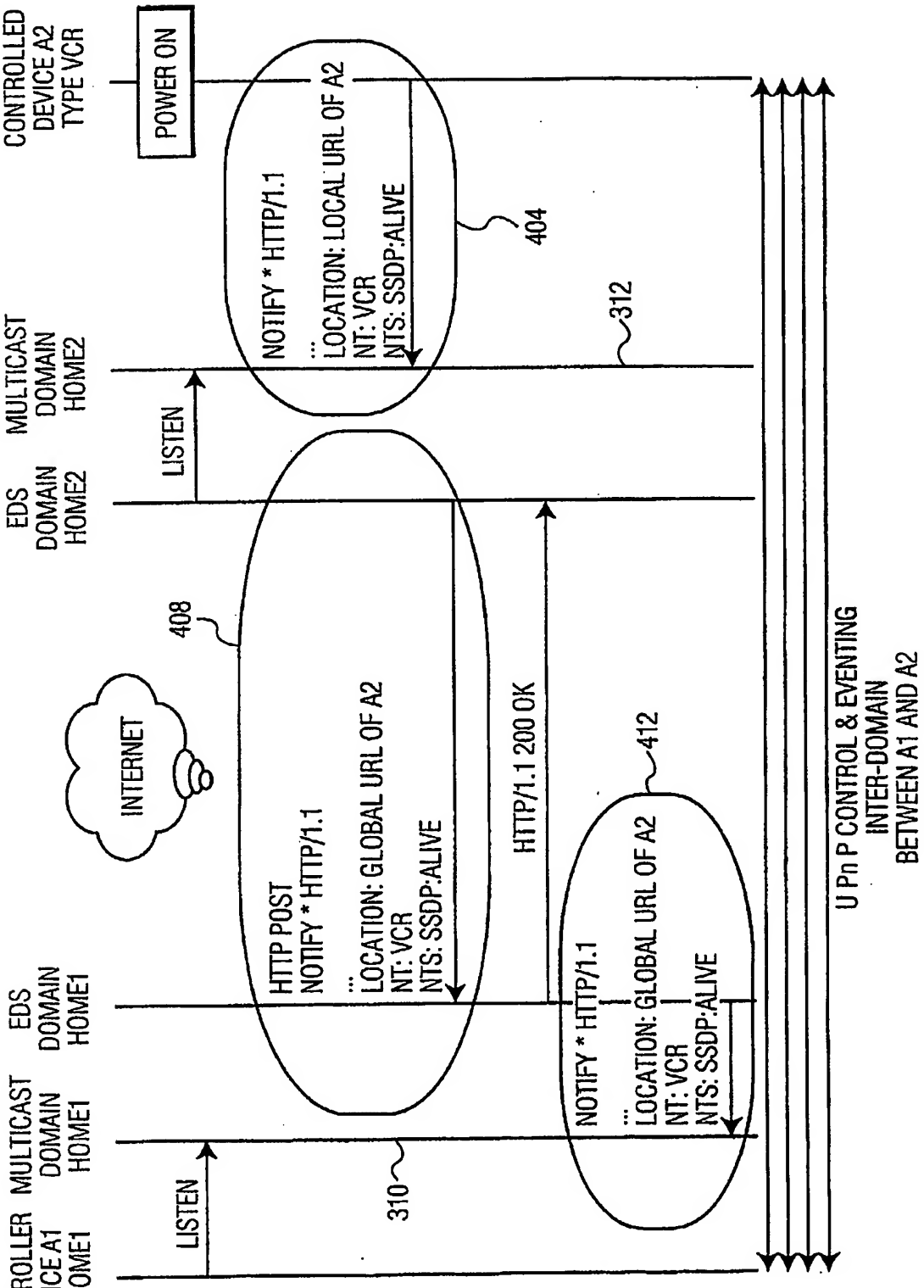

CONTROLLER DEVICE A1 IN HOME1
MULTICAST DOMAIN HOME1
EDS DOMAIN HOME1
EDS DOMAIN HOME2
MULTICAST DOMAIN HOME2
CONTROLLED DEVICE A2 TYPE VCR
LISTEN
LISTEN
POWER ON
INTERNET
310
312
404
408
412
HTTP POST
NOTIFY * HTTP/1.1
...
LOCATION: GLOBAL URL OF A2
NT: VCR
NTS: SSDP:ALIVE
HTTP/1.1 200 OK
NOTIFY * HTTP/1.1
...
LOCATION: GLOBAL URL OF A2
NT: VCR
NTS: SSDP:ALIVE
NOTIFY * HTTP/1.1
...
LOCATION: LOCAL URL OF A2
NT: VCR
NTS: SSDP:ALIVE
U Pn P CONTROL & EVENTING
INTER-DOMAIN
BETWEEN A1 AND A2

FIG. 6